1				
2				
3				
4				
5				
6				
7				
8	UNITED STATES DISTRICT COURT FOR THE WESTERN DISTRICT OF WASHINGTON			
9	AT SEATTLE			
10	DEDECCA COLICINEAU individually on hor	Cosa Na		
11	REBECCA COUSINEAU, individually on her own behalf and on behalf of all others	Case No.		
12	similarly situated,	CLASS ACTION COMPLAINT		
13	Plaintiff,			
14	v.			
15	MICROSOFT CORPORATION, a Delaware			
16	corporation,			
17	Defendant.			
18	PLAINTIFF'S CLASS ACTION COMPLAINT			
19	Plaintiff Rebecca Cousineau ("Plaintiff") brings this Class Action Complaint against			
20	Defendant Microsoft Corporation ("Microsoft" or "Defendant") based upon its practice of			
21	unlawfully tracking its users' geolocation information through their mobile devices. Plaintiff,			
22	for her Class Action Complaint, alleges as follows upon personal knowledge as to herself and			
23	her own acts and experiences and, as to all other matters, upon information and belief,			
24	including investigation conducted by her attorneys:			
25	NATURE OF THE ACTION			
26	1. Microsoft intentionally tracks the movements of its users' mobile devices in			
27	direct contravention of their privacy settings and the law. While Microsoft claims that users			
	COMPLAINT 1	TOUSLEY BRAIN STEPHENS PLLC 1700 Seventh Avenue, Suite 2200		

may opt-out of its location-tracking program, Microsoft has designed its mobile operating software to track its users locations deceptively even after they *affirmatively deny* such consent. As discussed more fully herein, Microsoft effectuates this scheme through its popular mobile operating system ("OS"), Windows Phone 7 ("Windows Phone"), which is used by a variety of manufacturers of mobile devices, such as HTC, Samsung, and LG. Regardless of the device model, Microsoft consciously designed its OS to siphon geographic location information from users and transmit their specific whereabouts to Microsoft's servers.

- 2. Over the past decade, mobile telephony use among United States consumers has grown exponentially. Seeking to capitalize on this new medium of communication, Microsoft is racing to develop a system that facilitates targeted advertisements to consumers based upon their geographic locations. Before Microsoft is able to effectuate such a marketing campaign, however, it must first compile a digital map by collecting geographic information and unique identifiers from cellular towers, wireless network routers, cellular telephones, and computer systems.
- 3. Faced with the expensive and laborious task of collecting this information, Microsoft has elected to gather instead, the necessary geolocation information through its customers' mobile devices. In this way, Microsoft uses its customers as a virtual army of surveyors who constantly gather and transmit the geolocation information necessary to build its digital map.
- 4. Microsoft's scheme is executed through its camera application, which comes standard with a mobile device running the Windows Phone OS. The first time a user opens the camera application, a display screen prompts the user to allow or deny Microsoft access to his or her geolocation:

26 ///

///

27 | ///

Allow the camera to use your location?
Sharing this information will add a location tag to your pictures so you can see where your pictures were taken. This information also helps us provide you with improved location services. We won't use the information to identify or contact you.
Privacy Statement allow cancel

(The above depiction is a true and accurate copy of the Windows Phone OS display screen ("Display Screen").)

- 5. Users clicking "cancel" explicitly deny Microsoft access to their geolocations. Unfortunately for its users, however, Microsoft brazenly continues to collect users' location information, regardless of whether or not the individual chooses "cancel" so as to not allow such information to be tracked. Thus, Microsoft surreptitiously forces even unwilling users into its non-stop geo-tracking program in the interest of developing its digital marketing grid.
- 6. Still, Microsoft publicly maintains that it only collects geolocation data "with the express consent of the user." (A true and accurate copy of Microsoft's Letter to Congress, dated May 9, 2011, is attached hereto as **Exhibit A.**). Nevertheless, and in clear contradiction to its assertions, Microsoft designed its camera application to transmit its users' geolocation information regularly to Microsoft's servers—even when the user expressly denies Microsoft access to such information.
- By and through these actions, Microsoft has refused and continues to refuse to honor its users' desire to refrain from being tracked.
- 8. By designing the Windows Phone camera application to thwart users' attempts to prohibit the collection of their geolocations, Microsoft blatantly disregards its users' privacy rights, and willfully violates numerous state and federal laws.

27 | ///

///

1 **PARTIES** 9. 2 Plaintiff Rebecca Cousineau is a natural person and citizen of the state of 3 Michigan. 10. 4 Defendant Microsoft Corporation is a Delaware corporation with its principal 5 place of business located at 1 Microsoft Way, in the city of Redmond, state of Washington. 6 **JURISDICTION AND VENUE** 7 11. This Court has jurisdiction over the subject matter of this action pursuant to 8 28 U.S.C. § 1331. This Court has personal jurisdiction over Defendant because it resides in 9 this District, conducts business in this District, and the improper conduct alleged in the 10 Complaint occurred in this District. 11 12. Venue is proper in this District under 28 U.S.C. § 1391(b) because Defendant 12 resides in this District, conducts business in this District, the improper conduct alleged in the 13 Complaint occurred in this District, and the injury arose in this District. Venue is additionally 14 proper because Defendant transacts significant business in this District. 15 **FACTUAL BACKGROUND** I. 16 Microsoft Profits from Collecting its Users' Location Data 13. 17 Mobile advertising is projected to become a \$2.5 billion dollar industry by 2015. To gain a competitive advantage, Microsoft is using mobile devices running the 18 19 Windows Phone OS to build a digital map, comprised of cell tower and wireless network 20 ("WiFi") access point information. (Ex. A, p 4.) In turn, this map can be used to help 21 pinpoint the location of users' mobile phones and other devices. 22 14. In the future, Microsoft can use its proprietary database of cell tower and WiFi 23 to deploy targeted advertisements to mobile phone users based upon their geolocations. 24 25 26 27 See, http://www.nytimes.com/2011/04/26/technology/26locate.html (last visited August 30, 2011).

- designed the Windows Phone OS to collect and send geolocation data to its servers when "a user-authorized application has made a request for location." (Ex. A, p. 4.)
- However, when consumers use certain Windows Phone OS mobile applications, they—regardless of their privacy restrictions—unwittingly transmit specific
- Previously, Microsoft had allowed public access to its database containing the approximate locations of millions of mobile phones, laptop computers, and other devices
- Strikingly, researchers were able to show that it is possible to track the approximate whereabouts of individual consumers using information gleaned from Microsoft's database.² Facing increased scrutiny over privacy concerns raised by the researchers' discovery, Microsoft recently ceased publication of the contents of its

- In April of 2011, leaders of the United States House of Representatives Committee on Energy and Commerce sent letters to a number of developers of mobile device operating systems, including Microsoft, requesting information about how their software was designed to track and store users' locations. In its response to Congress's inquiry, Microsoft unequivocally stated that the Windows Phone OS never collects geolocation data without the
- Specifically, Microsoft asserted that its OS will "collect data only if ... the user has allowed an application to access and use location data." (Ex. A, p. 4.)

See, Microsoft Curbs Wi-Fi Location Database, http://news.cnet.com/8301-31921_3-20086489-281/microsoft-curbs-wi-fi-location-database/ (last visited August 30, 2011).

individuals, defined as follows:

All persons in the United States that denied their Windows Phone 7 camera application access to their location information, and unwittingly had their geolocation data transmitted to Microsoft's servers.

Excluded from the Class are (1) Defendant, Defendant's agents, subsidiaries, parents, successors, predecessors, and any entity in which the Defendant or their parents have a controlling interest and their current and former employees, officers, and directors, (2) the Judge or Magistrate Judge to whom this case is assigned and the Judge's or Magistrate Judge's immediate family, (3) persons who execute and file a timely request for exclusion, (4) the legal representatives, successors, or assigns of any such excluded person, and (5) all persons who had claims similar to those alleged herein finally adjudicated or who have released their claims against Defendant.

- 29. **Numerosity:** The exact number of the members of the Class is unknown and is not available to Plaintiff at this time, but individual joinder in this case is impracticable. The Class consists of tens of thousands of individuals and other entities. Class members can be easily identified through Defendant's records and public records.
- 30. **Commonality:** There are many questions of law and fact common to the claims of Plaintiff and the other members of the Class, and those questions predominate over any questions that may affect individual members of the Class. Common questions for the Class include but are not limited to the following:
 - (a) Whether Microsoft continues to collect geolocation data through the camera application included in the Windows Phone 7 operating system when the user denies Microsoft access to that information;
 - (b) Whether Microsoft profits, or intends to profit from, the collection of geolocation data obtained as a result of the unlawful practices described more fully herein;
 - (c) Whether Microsoft's conduct described herein violates the Stored Communications Act, 18 U.S.C. §§ 2701, et seq.;

1	
2	
3	
4	
5	
6	
7	
8	
9	
10	
11	
12	
13	
14	
15	
16	
17	
18	
19	
20	
21	
22	
23	
24	
25	

provides the benefits of single adjudication, economy of scale, and comprehensive supervision by a single court. Economies of time, effort, and expense will be fostered and uniformity of decisions will be ensured.

34. **Policies Generally Applicable to the Class:** This class action is also appropriate for certification because Defendant has acted or refused to act on grounds generally applicable to the Class, thereby making appropriate final injunctive relief or corresponding declaratory relief with respect to the Class as a whole. The policies of the Defendant challenged herein apply to and affect all members of the Class uniformly, and Plaintiff's challenge of these policies hinges on Defendant's conduct, not on facts or law applicable only to Plaintiff.

FIRST CAUSE OF ACTION

Violations of the Stored Communications Act 18 U.S.C. §§ 2701, et seq. (On behalf of Plaintiff and the Class)

- 35. Plaintiff incorporates the foregoing allegations as if fully set forth herein.
- 36. The Electronic Communications Privacy Act, 18 U.S.C. §§ 2510, et seq. (the "ECPA") broadly defines an "electronic communication" as "any transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnetic, photoelectronic or photooptical system that affects interstate or foreign commerce...." 18 U.S.C. § 2510(12). The Stored Communications Act (the "SCA") incorporates this definition.
- 37. Pursuant to the ECPA and the SCA, "electronic storage" means any "temporary storage of a wire or electronic communication incidental to the electronic transmission thereof." 18 U.S.C. § 2510(17)(A). This type of electronic storage includes communications in intermediate electronic storage that have not yet been delivered to their intended recipient.

26

- 38. The SCA mandates, among other things, that it is unlawful for a person to obtain access to stored communications on another's computer system without authorization. 18 U.S.C. § 2701.
- 39. Congress expressly included provisions in the SCA to address this issue so as to prevent "unauthorized persons deliberately gaining access to, and sometimes tampering with, electronic or wire communications that are not intended to be available to the public." Senate Report No. 99–541, S. REP. 99-541, 35, 1986 U.S.C.C.A.N. 3555, 3589.
- 40. Microsoft has programmed its Windows Phone 7 operating system to store the location information ("the stored file") of its users. Microsoft has violated 18 U.S.C. § 2701(a)(1) because it intentionally accessed consumers' communications without authorization and obtained, altered, or prevented authorized access to a wire or electronic communication while in electronic storage by collecting location data from the stored file on Plaintiff and the Class's mobile devices while using the camera application, despite the fact that the user expressly denied Defendant access to that information. At all relevant times, Defendant had actual knowledge of, and benefited from, this practice.
- 41. Additionally, Defendant has violated 18 U.S.C. § 2701(a)(2) because it intentionally exceeded the authorization of consumers to access consumers' communications and obtained, altered, or prevented authorized access to a wire or electronic communication while in electronic storage by collecting location data from the stored file on Plaintiff and the Class's mobile devices while using the camera application, despite the fact that the user expressly denied Defendant access to that information. At all relevant times, Defendant had actual knowledge of, and benefited from, this practice.
- 42. As a result of Defendant's conduct described herein and its violation of § 2701, Plaintiff and the Class have suffered injuries. Plaintiff, on his own behalf and on behalf of the Class, seeks an order enjoining Defendant's conduct described herein and awarding himself and the Class the maximum statutory and punitive damages available under 18 U.S.C. § 2707.

SECOND CAUSE OF ACTION

Violations of the Electronic Communications Privacy Act 18 U.S.C. §§ 2510, et seq. (On behalf of Plaintiff and the Class)

- 43. Plaintiff incorporates the forgoing allegations as if fully set forth herein.
- 44. The Electronic Communications Privacy Act, 18 U.S.C. §§ 2510, et seq. (the "ECPA") broadly defines an "electronic communication" as "any transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnetic, photoelectronic or photooptical system that affects interstate or foreign commerce…" 18 U.S.C. § 2510(12).
- 45. The ECPA defines an "electronic communications system" as "any wire, radio, electromagnetic, photooptical or photoelectronic facilities for the transmission of wire or electronic communications, and any computer facilities or related electronic equipment for the electronic storage of such communications." 18 U.S.C. § 2510(14).
- 46. The ECPA broadly defines the contents of a communication. Pursuant to the ECPA, "contents" of a communication, when used with respect to any wire, oral, or electronic communications, include any information concerning the substance, purport, or meaning of that communication. 18 U.S.C. § 2510(8). "Contents," when used with respect to any wire or oral communication, includes any information concerning the identity of the parties to such communication or the existence, substance, purport, or meaning of that communication. The definition thus includes all aspects of the communication itself. No aspect, including the identity of the parties, the substance of the communication between them, or the fact of the communication itself, is excluded. The privacy of the communication to be protected is intended to be comprehensive.
- 47. Defendant's conduct violated 18 U.S.C. § 2511(1)(a) because Defendant endeavored to intercept and intentionally intercepted Plaintiff's and Class Members' electronic communications to, from, and within their mobile devices without consent.

- 48. Defendant's conduct violated 18 U.S.C. § 2511(1)(d) because Defendant endeavored to use and used the contents of Plaintiff's and Class Members' electronic communications to profit from its unauthorized collection and sale, knowing and having reason to know that the information was obtained through interception in violation of 18 U.S.C. § 2511(1).
- 49. Defendant intentionally obtained and/or intercepted, by device or otherwise, these electronic communications, without the knowledge, consent or authorization of Plaintiff or the Class.
- 50. Plaintiff and the Class suffered harm as a result of Defendant's violations of the ECPA, and therefore seek (a) preliminary, equitable and declaratory relief as may be appropriate, (b) the sum of the actual damages suffered and the profits obtained by Defendant as a result of their unlawful conduct, or statutory damages as authorized by 18 U.S.C. § 2520(2)(B), whichever is greater, (c) punitive damages, and (d) reasonable costs and attorneys' fees.

THIRD CAUSE OF ACTION

Violations of the Washington Consumer Protection Act RCW 19.86, et seq. (On behalf of Plaintiff and the Class)

- 51. Plaintiff incorporates by reference the foregoing allegations.
- 52. Washington's Consumer Protection Act, RCW § 19.86, *et seq.* ("CPA") protects both consumers and competitors by promoting fair competition in commercial markets for goods and services.
- 53. The CPA prohibits any unlawful, unfair or fraudulent business acts or practices including the employment of any deception, fraud, false pretense, false promise, misrepresentation, or the concealment, suppression, or omission of any material fact.
- 54. As described herein, Microsoft's continued unlawful and unconscionable conduct of transmitting geolocation data after the user has expressly denied Microsoft access

to such information constitutes an unlawful business practice in violation of RCW § 19.86, et seq.

- 55. By doing so, Microsoft engaged, and continues to engage, in a deceptive and misleading course of conduct intended to deceive and significantly confuse consumers into purchasing its software (via purchasing any Windows Phone) and using its applications (*i.e.*, its Windows Phone camera application) which constitutes unconscionable commercial practices, deception, fraud, false promises, false pretenses and/or misrepresentations in its interactions with Plaintiff and the Class.
- 56. The ability to control the privacy settings of a consumer product (*i.e.*, access to geolocation information) is material to any transaction because it is likely to affect a consumer's choice of, or conduct regarding, whether to purchase a product. Any deception related to the privacy settings of a consumer product is materially misleading.
- 57. The misrepresentation of the privacy settings of Microsoft's products is likely to mislead a reasonable consumer who is acting reasonably under the circumstances.
- 58. Microsoft has violated the "unfair" prong of the CPA in that their actions caused substantial injury to consumers by failing to disclose that it was accessing consumers' geolocation information after the user has expressly denied Microsoft access to such information. The injury caused by Microsoft's conduct is not outweighed by any countervailing benefits to consumers or competition, and the injury is one that consumers themselves could not reasonably have avoided.
- 59. The act and practice of Microsoft is injurious to the public interest because Microsoft has injured numerous people beyond just Plaintiff. Microsoft has the ongoing capacity to injure members of the public through the conduct alleged in this Complaint.
- 60. Microsoft also violated the CPA by engaging in fraudulent and/or deceptive conduct by representing that it would honor its users' decisions not to have location data recorded and sent to its servers.

68. While Plaintiff and the Class did not purchase their Windows Phones directly

by purchasing a mobile device with the Windows Phone 7 OS that Microsoft claimed would

not transmit geolocation data without the express consent of the user.

25

26

mobile devices after the user has expressly denied access to that information;

1	D.	Award damages, inclu	iding statutory damages of \$1,000 per violation under	
2	the Stored Co	ommunications Act, 18 U	U.S.C. § 2707(c) and the Electronic Communications	
3	Privacy Act,	18 U.S.C. § 2520, and p	unitive damages where applicable, to Plaintiff and the	
4	Class in an a	Class in an amount to be determined at trial;		
5	E.	Award Plaintiff and th	e Class their reasonable litigation expenses and	
6	attorneys' fees;			
7	F.	Award Plaintiff and th	ne Class pre- and post-judgment interest, to the extent	
8	allowable; and			
9	G.	Award such other and	further relief as equity and justice may require.	
10	JURY TRIAL			
11		Plaintiff demands	a trial by jury for all issues so triable.	
12				
13				
14	Dated: Augu	st 31, 2011	Respectfully submitted,	
15			TOUSLEY BRAIN STEPHENS PLLC	
16			By: /s/ Kim D. Stephens	
17			Kim D. Stephens, WSBA #11984 1700 Seventh Avenue, Suite 2200	
18			Seattle, Washington 98101	
			Telephone: (206) 682-5600	
19			Facsimile: (206) 682-2992 kstephens@tousley.com	
20			-	
21			Jay Edelson (pro hac admission pending) Rafey S. Balabanian (pro hac admission	
22			pending) William C. Gray (pro hac admission pending)	
23			Ari J. Scharg (pro hac admission pending)	
24			EDELSON MCGUIRE, LLC 350 North LaSalle Street, Suite 1300	
25			Chicago, Illinois 60654 Telephone: (312) 589-6370	
26			Facsimile: (312) 589-6378	
27				

1	jedelson@edelson.com rbalabanian@edelson.com
2	wgray@edelson.com ascharg@edelson.com
3	*Pro hac vice admissions to be sought
4	Counsel for Rebecca Cousineau and the
5	Putative Class
6	
7	
8	
9	
10	
11	
12	
13	
14	
15	
16	
17	
18	
19	
20	
21	
22	
23	
24	
25	
2627	
21	